AFFIDAVIT OF SPECIAL AGENT JOSEPH IANNACCONE IN SUPPORT OF AN APPLICATION FOR A CRIMINAL COMPLAINT

I, Joseph Iannaccone, Special Agent with the Department of Homeland Security, Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI") since 2009, and am currently assigned to the office of the Special Agent in Charge, Boston, MA. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training and everyday work related to these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. § 2252A, and I am authorized by law to request a search warrant.

2. I submit this affidavit in support of a criminal complaint charging James TALLACH, YOB 1968, a Scottish citizen of the United Kingdom living in Malden, Massachusetts, with one count each of distribution and receipt of child pornography, in violation of 18 U.S.C. § 2252A(a)(2)(A), and one count of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B).

3. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. Because this affidavit is submitted for the limited purpose of establishing probable cause

to secure a criminal complaint, I have not included each and every fact known to me concerning the investigations generally outlined below.

STATEMENT OF PROBABLE CAUSE

A. The HSI Investigation

4. In October 2015, HSI agents in Arizona began conducting undercover operations on an Internet-based video conferencing application, hereinafter referred to as "Application A,"[1] which law enforcement had discovered was being used by persons to facilitate the exchange of child pornography.

5. "Application A" is an internet-based video conferencing tool which allows users to connect via the internet to participate in a virtual conference room. "Application A" permits users to conduct online video conferences without charge for a limited number of minutes. Paid subscribers can conduct online video conferences for an unlimited amount of time. Some "Application A" users with a paid account permit their rooms to be accessed without a password such that anyone who knows the room number can enter and leave the room at any time.

6. "Application A" is designed for video conferencing on multiple device formats. To use this application, a user downloads the application to a computer, mobile phone, or other mobile device (e.g., tablet) via direct download from the company's website. Once downloaded and installed, the user is prompted to create an account. "Application A" users can invite others to an online "meeting room," which is an online location associated with a 10-digit number where each user can see and interact with the other users.

[1] The actual name of "Application A" is known to law enforcement. "Application A" remains active and disclosure of the name of the application would potentially alert its users to the fact that law enforcement action is being taken against users of the application, thereby provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, to protect the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the application will be identified herein as "Application A."

7. When a user chooses to enter a specific meeting room, the user enters the 10-digit room number and enters the username that he wants to use on that specific occasion, which does not have to be the same as the account username. "Application A" does not require a certain number of characters for a particular username. Consequently, a user can create a name with a single special character, such as "#," or a single letter, such as "a."

8. During a meeting, users can show a live image or video of themselves to other users through the webcam feature of their device. Users may also display the contents of their own computer desktops to the other users in the room. The ability to display their own computer desktops allows users to show videos and photos to other users in the room. "Application A" also allows users to send text messages visible to all of the users in the room, or private messages that are similar to instant messages sent between two users.

9. Within each virtual conference room, there are three sections visible on a user's screen: video/live camera streaming, group chat, and the participant section, which shows all active participants within the virtual meeting room at a given time. A user participating in a given meeting room would be able to see the following items:

   a. The video/live streaming function, which covers the left hand side of the screen;

   b. The chat room/private message function, which is displayed on the top right hand side of the screen;

   c. A list of participants in the virtual conference room at that time, which is beneath the chat section on the bottom right hand side of the screen and which indicates with icons next to each participant name whether he has microphone and/or camera capabilities; and

   d. Seven icons on the bottom of the screen, which are labeled: 1. Join Audio, 2. Start Video, 3. Invite, 4. Participants, 5. Share Screen, 6. Chat, and 7. Leave Room.

10. Participants can take an active role during a virtual meeting by either participating in the chat or by live-streaming video through their web camera. "Application A" allows the user to live-stream his web camera or to play pre-recorded videos – or he may deactivate his microphone and web camera and still remain a participant in the meeting room. Users have the ability to scroll through participating camera feeds and may select to focus on any particular streaming video or live web camera that is active at any given time. When users live stream their web cameras or pre-recorded video, their display names appear on the bottom left hand corner of their video feed. The number of video feeds displayed within the application (arranged as tiles) depends on how many camera feeds each user chooses to monitor.

11. "Application A" maintains IP address[2] logs for each meeting room, which include all of the IP addresses (and related usernames) for each user in a particular room on a specific day and the device that was used by each user. Each user's unique IP address is logged to reflect the time that particular user entered the room and the time the user exited the room. Users can enter and exit the room multiple times, thereby creating multiple sessions[3] within the logs of "Application A." In other words, if a room is open and active for one hour, and in that hour, a user enters the room, leaves the room, and then re-enters the room, the "Application A" IP log records would reflect two sessions for that specific user (entry/exit, followed by second entry) in the same room on that date.

---

[2] An Internet Protocol (IP) address is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication. Computers on the Internet identify each other by an IP address. IP addresses can assist law enforcement in finding a particular computer on the Internet. IP addresses can typically lead law enforcement to a particular Internet service company and that company can typically identify the account that used the IP address to access the internet.

[3] As used herein, a session refers to a particular user's time in a specific "Application A" room.

12. Between January 9, 2017 and February 6, 2018, an HSI agent acting in an undercover capacity and using a device connected to the Internet signed into an "Application A" user account and entered an "Application A" meeting room ("MEETING ROOM"). On each of those dates, the agent observed that a user in the MEETING ROOM with the display name "Sean Scot" or "twsTs prv" displayed or streamed videos depicting child pornography, i.e., visual depictions of minors engaging in sexually explicit conduct, which were visible to the other users in the room. The undercover agent was able to record these child pornography videos, messages, and other activity in the MEETING ROOM to an undercover device.

13. I have viewed the child pornography videos that a user with the display name "Sean Scot" and "twsTs prv" transmitted to other users of "Application A" in sessions that have been provided to me from HSI Phoenix. They include the following:

a. On April 4, 2017, a user with the display name "Sean Scot," who was listed as the host of the MEETING ROOM, streamed multiple video clips containing what I believe to be child pornography, including videos of children from infancy to approximately ten years of age being penetrated anally and vaginally. One clip, which streamed from approximately 6:04 PM UTC to 6:05 PM UTC, depicts a boy who appears to be approximately three years old positioned face down on a couch by an adult male, who is shown anally penetrating the child with his erect penis from behind. While this video was playing, "Sean Scot's" webcam was activated and captured his face[4] and torso area.[5]

---

[4] Based on my review of images of TALLACH maintained by the Registry of Motor Vehicles, in publicly-accessible social media, and in Massachusetts State Police booking documents, I believe that the user depicted was TALLACH.

[5] Still images from this video are available for this Court's review.

b. On February 6, 2018, a user with the display name "twsTs prv" streamed multiple video clips containing what I believe to be child pornography. Text visible to the undercover agent indicates "You are viewing twsTs prv's screen." The host's webcam is turned on, showing an adult male laying on a bed, masturbating, with the bottom half of his face (and white goatee) visible.[6] Chat text captured by the undercover agent includes a user asking, "is that you sean scot? lol" and "twsTs prv" responding, "yep!!" One of the clips that "twsTs prv" streamed for approximately 19 seconds depicts a female child who appears to be approximately two years old putting the erect penis of an adult male into her mouth. The naked adult male is seated on a couch, and visible in the frame near him is a mouse pad with the word "Dad" written on it.[7]

B. The Massachusetts State Police Investigation

14. On or about May 16, 2018, the Massachusetts State Police (MSP) Internet Crimes Against Children (ICAC) Task Force received a CyberTipline Report, numbered 28380594, from the National Center for Missing and Exploited Children (NCMEC).[8] The CyberTipline Report, submitted by the ESP Multi Media, LLC/Zmedianow, LLC/Chaturbate, identified

---

[6] In the image of TALLACH described in paragraph 13(a), TALLACH sports a similar goatee.

[7] Still images from this video are available for this Court's review.

[8] NCMEC is a nonprofit organization that serves as the nation's clearinghouse and reporting center for all issues related to the prevention of and recovery from child victimization. See www.missingkids.com/home, last accessed July 25, 2018. Electronic Service Providers (ESPs) are required to report apparent violations of laws prohibiting the possession, receipt, distribution, and production of child pornography to NCMEC's CyberTipline. 18 U.S.C. § 2258A(a). Such CyberTipline reports must include information within the ESP's custody and control regarding the identity of the involved individual(s), information regarding the geographic location of the involved individual(s), any images of apparent child pornography, and the complete communication containing any images of apparent child pornography. 18 U.S.C. § 2258A(b). NCMEC is required by law to forward each CyberTipline report to appropriate state or federal authorities. 18 U.S.C. § 2258A(c).

an incident of apparent child pornography by an individual with the screen/username "Sean Scot" on March 2, 2018, and identified the user's IP address as 96.230.24.7.

15. On or about May 16, 2018, MSP ICAC received two additional CyberTipline Reports from NCMEC. Report number 16067357 was filed with NCMEC by the ESP Skype.com on or about December 19, 2016 regarding an incident of apparent child pornography by an individual with the screen/username "seanscot1" from the IP address 100.0.242.28. Report number 16292009 was filed with NCMEC by the ESP tumblr.com on or about July 23, 2016 regarding an incident of apparent child pornography by an individual with the screen/username "btmbud" and an associated email address of "jamesscotman1@gmail.com," from the IP address 71.184.152.211.

16. Investigators determined that all three aforementioned IP addresses resolved to Verizon. In response to subpoenas from the Massachusetts Attorney General's Office, Verizon provided records regarding the subscriber information for each of the IP addresses. The customer name in each instance was reported as James TALLACH, at 33 Lanark Road in Malden, Massachusetts.

17. Based on the information set forth above, MSP ICAC obtained a warrant from the Malden District Court, docketed as 185OSW76, to search 33 Lanark Road, Floor 2, Malden, Massachusetts for evidence, fruits, and instrumentalities of violations of state child pornography laws.

18. On May 30, 2018, members of MSP ICAC, along with members of the Malden Police Department, executed the above-referenced search warrant. TALLACH was present and was provided with provided a copy of the warrant, and spontaneously commented that he uses Chaturbate, not Skype, and had just recently installed Tumblr.

19. During the execution of the search warrant, investigators seized approximately eight items, including four computers, a cell phone, two tablets, and one electronic storage device. The forensic analysis of those items is in process by MSP ICAC.

20. To date, forensic analysis of one computer, an HP Envy x360 laptop recovered from TALLACH's room, has revealed approximately 291 files that investigators believe, based on their training and experience, contain child pornography, including videos and images of prepubescent children, including toddlers, involved in sexual conduct with adult men. Included among those files is the following:

a. (toddlerboy) artem 3yo-cum.mp4 - This video is approximately two minutes and five seconds in length and depicts an adult male rubbing his erect penis against the penis and testicles of a boy who appears to be approximately two to three years old. Towards the end of the video, the adult male ejaculates semen on the toddler's penis and testicles.[9] This video was located at file path G:\$recyclebin\s-1-5-21-1599804547-1357852909-3285897690-1004\$r11teq3\beast\absolutefavorites\(toddlerboy) artem 3yo-cum.mp4. Data accessible to agents through forensic examination indicates an "accessed" date of May 13, 2018 and a "created" date of May 13, 2018, which indicates a strong probability that the video was downloaded on May 13, 2018.

b. $rrzieye – This video is approximately two minutes and 19 seconds in length and depicts the vagina and upper legs of a nude infant whose anus is being penetrated by an adult male's penis. Towards the end of the video, the male rubs his penis on the child's vagina and ejaculates onto the child's stomach.[10]

[9] Still images from this video are available for the Court's review.

[10] Still images from this video are available for the Court's review.

21. Forensic analysis of the HP laptop to date has also revealed evidence of the use of "Application A" and the Chaturbate user accounts "seanscot" and "twsTdprv."

CONCLUSION

22. Based on the foregoing, I submit that there is probable cause to believe that:

a. On or about April 4, 2017 and February 6, 2018, TALLACH knowingly distributed, and attempted to distribute, any child pornography that had been mailed, shipped, and transported in and affecting interstate and foreign commerce by any means, including by computer, in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1); and

b. On or about May 13, 2018, TALLACH knowingly received, and attempted to receive, any child pornography that had been mailed, shipped, and transported in and affecting interstate and foreign commerce by any means, including by computer, in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1); and

c. On or about May 30, 2018, TALLACH knowingly possessed any material that contained one and more images of child pornography that had been mailed, shipped, and transported using any means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce by any means, including by computer, and that was produced using materials that had been mailed, and shipped and transported in and affecting interstate and foreign commerce by any means, including by computer, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2).

Sworn to under the pains and penalties of perjury,

Joseph Iannaccone
Special Agent
Homeland Security Investigations

SUBSCRIBED and SWORN to before me on July 25th, 2018.

HONORABLE MARIANNE B. BOWLER
UNITED STATES MAGISTRATE JUDGE

I have reviewed still images from the videos described in paragraphs 13 and 20 above, and I find probable cause to believe that the images depict minors engaged in sexually explicit conduct. The Affiant shall preserve said images for the duration of the pendency of this matter, including any relevant appeal process.

HONORABLE MARIANNE B. BOWLER
UNITED STATES MAGISTRATE JUDGE